Workspace ONE and Android Enterprise

Meet any enterprise use case simply and securely

At a glance

The combination of VMware Workspace ONE® and Android empowers the anywhere workforce with a secure and consumer-friendly experience to transform how work gets done.

Key benefits

- Easily configure and deploy personal and company-owned Android devices
- Configure enterprise security and end-user privacy for work apps and data from one console
- Deliver unified access to all apps, including Android apps with Google Play integration

Whether at home, at the office, in the field or on the go, mobile devices enable employees to be connected and productive regardless of location. And their uses are expanding to include even the most mission-critical operations of an organization. The increasing availability of modern, mobile applications and the demand for off-network connectivity creates challenges for IT in terms of management, data security and digital employee experience.

The VMware Workspace ONE platform combines app delivery, access control and unified endpoint management (UEM). IT can configure device policies, manage apps and gain data-driven insights about their device fleet from a unified console. For users, the Workspace ONE Intelligent Hub app delivers a personalized experience through self-service access to remote support, the corporate directory, IT and HR communications, and a centralized app catalog. To streamline the experience even more, IT can enable single sign-on (SSO) for fast and password-less access to work-critical resources.

Workspace ONE business mobility on Android devices

The Android operating system powers many types of devices: smartphones, tablets, wearables and ruggedized devices. Android Enterprise maintains a consistent experience for end users, regardless of device manufacturer and form factor. It also provides a modern management approach for enterprises and offers multiple deployment modes to suit a wide variety of use cases.

Workspace ONE UEM support for Android Enterprise deployment modes

Both employee privacy and company security are a concern for bring-your-own-device (BYOD) deployments. With Workspace ONE, you can deliver a work profile to separate work apps and data on the device. Work apps are badged with an icon to visually signify to the end user which apps are managed by your organization. Employees can turn off their work profile to stop receiving work notifications at the end of the day or when they are on vacation.

For greater control and security, organizations can provision corporate devices in fully managed device mode. IT can lock fully managed devices into a single app or multiple apps for dedicated device uses. The managed Google Play store on these devices is restricted to only corporate-allowed apps. Offering maximum enrollment flexibility, Workspace ONE UEM integrates with different methods of onboarding—QR code, NFC bump, EMM identifier, zero-touch enrollment, and Samsung Knox Mobile Enrollment.

Organizations can also enable a work profile for corporate-owned, personally enabled (COPE) use cases. This deployment mode delivers badged corporate apps in the work profile and gives the end user the ability to install personal apps outside of the work profile.

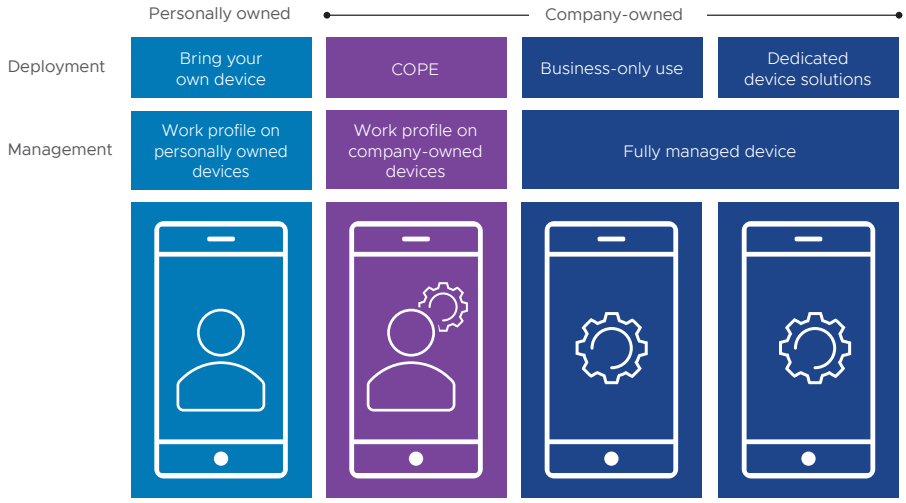

Figure 1: Flexible device management offers IT choices.

Secure management of devices from one console

The unified Workspace ONE UEM console is where admins integrate with Google to configure Android devices to deploy the work profile and device settings (fully managed or COPE). Admins can also monitor the entire device fleet. Workspace ONE Intelligence delivers rich visualizations and automations to help improve the digital employee experience and strengthen security. With the automated compliance engine, rooted or noncompliant devices can be remediated with actions, such as sending notifications or wiping the device. When a work profile is deployed, admins can set policies, such as restricting the user from sharing data from a managed app to a personal app. Work-managed applications can require a separate and more complex passcode for authentication while users can still access their personal information with their device passcode. With VMware Workspace ONE Assist, IT and help desk staff can remotely view or control any Android device directly from the Workspace ONE console while maintaining employee privacy and trust.

Workspace ONE with Android Enterprise also enables dedicated-device use cases, such as rugged devices and kiosks. Devices can even be configured for shared device mode, enabling users, such as shift workers, to check devices in and out and get access to their assigned apps and resources. Workspace ONE Launcher enables fully customizable experiences on shared Android devices to ensure that users have access to the apps and resources they need, when they need them.

Learn more

Visit vmware.com/products/workspace-one, or call +1-877-4-VMWARE.

Single location for all apps

VMware Workspace ONE Intelligent Hub provides a self-service catalog for all applications, including web, SaaS, and virtual and managed Android native apps. Workspace ONE integrates with Google Play both in the Workspace ONE UEM console and on the device for a truly seamless experience for both the admin and the end user. Google Play is embedded in the admin console, so the admin does not need to navigate to another location to approve work applications.

In addition, IT can provide a consumer-simple Workspace ONE suite of productivity apps for email, calendar, contacts and content that also protects critical work resources with data loss prevention policies.

Workspace ONE establishes trust between the user, device and enterprise for one-touch authentication into work apps for a secure and seamless experience. End users can navigate to their centralized app catalog and gain instant access to their work data. You can apply SSO to the installed managed applications. Workspace ONE can enforce authentication strength and restrict access to noncompliant devices.

Item No: FY23-6772-VMW-EMPOWER-ANYWHERE-WORKFORCE-ANDROID-ENTERPRISE-DS-USLET-WEB-20220401 4/22